A Blockchain-based Trading Matching Scheme in Energy Internet

Xin Lu
School of Control and Computer Engineering, North China Electric Power University
Beijing, China
13051320793@163.com

Zhitao Guan
School of Control and Computer Engineering, North China Electric Power University
Beijing, China
guan@ncepu.edu.cn

ABSTRACT
With the advent of the Industry 4.0 era, the energy industry system revolution will also face new challenges. Against the backdrop of the global energy crisis, renewable energy has received great attention from countries around the world. Due to the characteristics of geographical dispersion, randomness, volatility and uncontrollability of renewable energy, the centralized traditional electrical energy networks cannot meet the management requirements of large-scale access to renewable energy. The emergence of the energy internet has enabled the effective use of renewable energy. As a distributed trading and data management technology, blockchain solves the problem of distributed electrical energy trading in the energy Internet. However, the distributed energy trading based on blockchain cannot satisfy the rational matching of trading objects. Therefore, we propose a blockchain-based electrical energy trading system BC-TMS Blockchain-based trading matching system, which can reasonably match trading objects according to the user's personalized needs and maximize the benefits of both parties to the trading. At the same time, the system also provides a certain degree of privacy protection. Finally, through security and application prospect analysis, we prove the usability and practicability of our proposed scheme.

KEYWORDS
Energy Internet, Blockchain, Trading matching, Privacy Protection

ACM Reference Format:
Xin Lu and Zhitao Guan. 2020. A Blockchain-based Trading Matching Scheme in Energy Internet. In *2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI'20), October 5, 2020, Taipei, Taiwan.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3384943.3409430

ACM ISBN 978-1-4503-7610-5/20/10...$15.00
https://doi.org/10.1145/3384943.3409430

1 INTRODUCTION
Today, Industry 4.0 [1] has received widespread attention from both academia and industry. Industry 4.0 combines the Information Technology (IT) and the Operational Technology (OT), and transitions from a traditional centralized control model to an enhanced decentralized control model. Industry 4.0 integrates different technologies such as Cyber-Physical Systems (CPS), Industrial Internet of Things (IIoT), and Edge Computing infrastructures (Cloud/fog computing systems) in the industrial systems with the goal of creating a high efficiency, automated and Intelligent production and sales model mode. Under this model, traditional industry and technology boundaries will gradually fade, and new industries and forms of cooperation will emerge. As a consequence, the process of value creation will be changed and the division of industry chain will be reorganized.

Under the technical framework of Industry 4.0, the energy structure is changing. The distributed energy architecture of the Energy Internet enables large-scale access to distributed clean energy over a wide area. The energy internet framework is shown in Fig 1. The Energy Internet combines cutting-edge electronic technology, information technology and automation management technology to realize the interconnection of distributed energy production equipment, distributed energy storage equipment and distributed communication equipment to form an energy node and establish a huge energy network. Various loads realize bidirectional flow of energy, peer-to-peer exchange and sharing network [2].

As technology advanced, critical infrastructures increasingly come to rely on digital control systems and networking. In the Energy Internet, secure distributed energy trading methods have been widely concerned by academia and industry. In recent years, blockchain has become increasingly popular as a decentralized transaction and data management technology. The reason for the interest in Blockchain is its central attributes that provide security, anonymity and data integrity without any third-party organization in control of the trading, and therefore it is applied in numerous fields. Contemporarily, Blockchain can offer cryptography for transactions and data in trustless distributed networks to enhance the reliability and resilience of the critical infrastructure. In other words, increasingly open and security needs is forcing us to shore up defenses with developing blockchain technology to help secure distributed critical infrastructure. The technical advantages of the blockchain are undoubtedly very

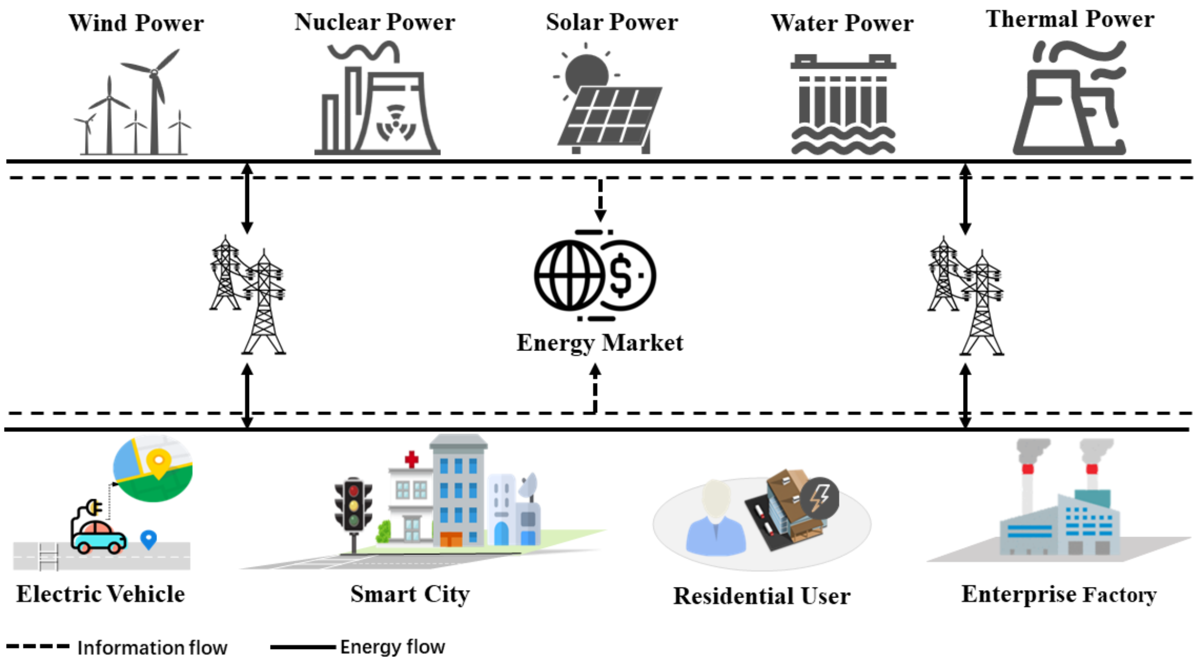

Figure 1: Energy Internet Trading Architecture.

suitable for the distributed trading environment of the energy Internet.

Blockchain can offer cryptography for trading and data in trustless distributed networks to enhance the reliability and resilience of the critical infrastructure [3]. In this scene, the question remains on how we can utilize blockchain techniques to secure critical infrastructure. Although the blockchain provides a secure trading architecture, there are still two key issues to be resolved. First, in a decentralized environment, how to achieve accurate matching of trading users according to user needs is a key issue of research. Secondly, how the blockchain as a distributed ledger open to the entire network can achieve user privacy protection during the trading matching phase. These two problems have undoubtedly become the defects of the distributed trading system based on blockchain.

In order to solve the problem of trading object matching and privacy protection in distributed energy trading based on blockchain, we have fully analyzed the operation mode and operation process of the distributed trading market. On this basis, we establish the trading matching model BC-TMS with the goal of the highest satisfaction and the maximization of benefits. At the same time, we introduce the idea of agency into electronic trading, using the virtual agent node of the blockchain to act as the identity of the agent, assisting the buyers and sellers of the network to match trading. This black box operation design achieves high-efficiency and low-cost trading matching while ensuring fairness and meeting privacy protection requirements. Our main contributions are as follows:

- We have proposed a distributed energy trading matching scheme BC-TMS based on blockchain. The scheme introduces the concept of satisfaction. Trading users can customize soft constraints and hard according to their needs to express their trading preferences. BC-TMS introduces a matching algorithm to match users with the highest satisfaction of trading objects, and achieves reasonable and accurate matching between buyers and sellers. This design not only improves the fairness of the trading but also maximizes the benefits.
- BC-TMS achieves high-efficiency and low-cost trading matching and privacy protection by introducing agent nodes. In the traditional blockchain system, most of the nodes publish trading intention information through network broadcasting. This method not only causes a lot of communication overhead, but also the user's Private data cannot be effectively protected. The introduction of the agent node makes the transaction matching process a black box operation, and the node cannot steal private information.
- Finally, we conducted a detailed security analysis and practical application mode analysis of BC-TMS. Through multi-dimensional analysis and discussion, we have reached the final conclusion. The analysis result proves that the security of our proposed BC-TMS system

meets the design requirements. At the same time, we made a comparative summary of similar distributed renewable energy trading systems based on blockchain. The results show that our proposed system is indeed practical.

The chapters of the paper are organized as follows. In the section 2, we will summarize, compare and analyze related work. In the section 3, we will present the system model and design goals. In the section 4, We will introduce the algorithm flow of BC-TMS in detail. Section 5 will analyze the security of the system algorithm. In the section 6, we have demonstrated the application prospects. Section 7 concludes the paper.

2 RELATED WORK

Industry 4.0 brings new opportunities and challenges to the reform of traditional industrial systems. Many researchers have been working on both the conceptual development and practical applications of Industry 4.0. Lu et al. [4] conducted a comprehensive analysis and summarization from the concept, architecture and application of Industry 4.0. Zhou et al. [5] conducted an in-depth discussion on the strategic planning, key technologies, opportunities and challenges of Industry 4.0. There are also other applications of Industry 4.0 in [6][7]. It is not difficult to see from the above research that the energy Internet discussed in this paper is undoubtedly one of the important industrial applications in the context of Industry 4.0.

Energy Internet [8] is developing rapidly as one of the most important industrial systems in the Industrial 4.0 era. In recent years, a large number of research on Energy Internet has provided new directions for solving the inherent defects of the Energy Internet. Paper [9] established the relationship between urban development and urban energy system through the improved LEAP model. According to the development trend of urban energy system, the connotation, composition and framework of urban energy internet are pointed out. Li et al. proposed a decentralized on-demand energy supply method based on microgrid to provide decentralized on-demand energy for mining in IoT devices [10]. The scheme proposes an energy supply structure to meet the different energy requirements of miners for different consensus agreements. In [11], Wang et al. comprehensively analyzed the architecture, methods and technologies of the Energy Internet. [12] Discussed the stability of the Energy Internet system and performed big data analysis on how to maintain a stable and healthy energy network environment. This type of research promotes the rapid development of the Energy Internet. It comprehensively analyzes the architecture, methods, and technologies of the Energy Internet, and provides the foundation for our research on the Energy Internet.

In the Energy Internet, distributed energy trading has always been a hot issue of concern. As a distributed ledger, blockchain is widely used in the Energy Internet by virtue of its technical advantages. BAZA et al. leverage the blockchain and smart contracts to build a decentralized charging coordination mechanism without the need for a centralized charging coordinator [13]. For the vehicle-mounted energy network (VEN), the paper [14] proposed a blockchain-based VEN energy transmission safety incentive scheme. This scheme introduces a novel energy blockchain system to achieve a safe energy transmission incentive scheme between nodes. Su et al. proposed a contract-based energy blockchain for safe electric vehicle charging services in smart communities [15]. This scheme solves the problem of how to optimally schedule the charging behavior of electric vehicles with different energy consumption preferences in a smart community. Paper [16] developed an optimization model and blockchain-based architecture to manage the operation of crowdsourced energy systems (CES) through peer-to-peer (P2P) energy trading transactions (ETTs). Wang et al. [17] conducted a detailed survey and a classification of existing blockchain-based energy trading schemes in the power system . Kang et al. [18] proposed a localized p2p electric vehicle energy trading scheme based on the consortium chain, which uses the iterative double auction mechanism to maximize the social welfare in the transaction. Yang et al. [19] introduced the application of blockchain in the future Energy Internet distributed environment. Mengelkamp et al. [20] proposed a sustainable blockchain-based smart grid for the local energy market. The above scheme has realized the blockchain-based energy trading.

Although there have been many researches on distributed energy trading based on blockchain, there is not much focus on trading matching. The popularity of mobile devices has driven the emergence of ultra-dense wireless networks (UDNs). Seng et al. developed an effective task-VM matching algorithm that takes into account task execution time and energy consumption [21]. The paper [22] proposed the hawk framework, and implemented a trading matching model based on the auction mechanism through smart contract technology. As a general trading matching model, Hawk also implements privacy protection. In addition, there is also a lot of research work on matching algorithms and models. Liang et al. proposed a matching model for multi-address network users [23]. kbarpour et al. research on trading matching methods in dynamic markets [24]. From the above research, it is not difficult to conclude that the research on the trading matching method based on blockchain technology is of great significance.

3 MODELS AND GOALS

In this section, we will give an overview of the expected goals and system model.

3.1 Design Goals

The distributed energy trading based on blockchain largely solves the circulation and utilization of distributed energy in the energy internet. However, the discrete nature of the distributed environment makes it difficult to find potential trading objects. At the same time, this process will consume

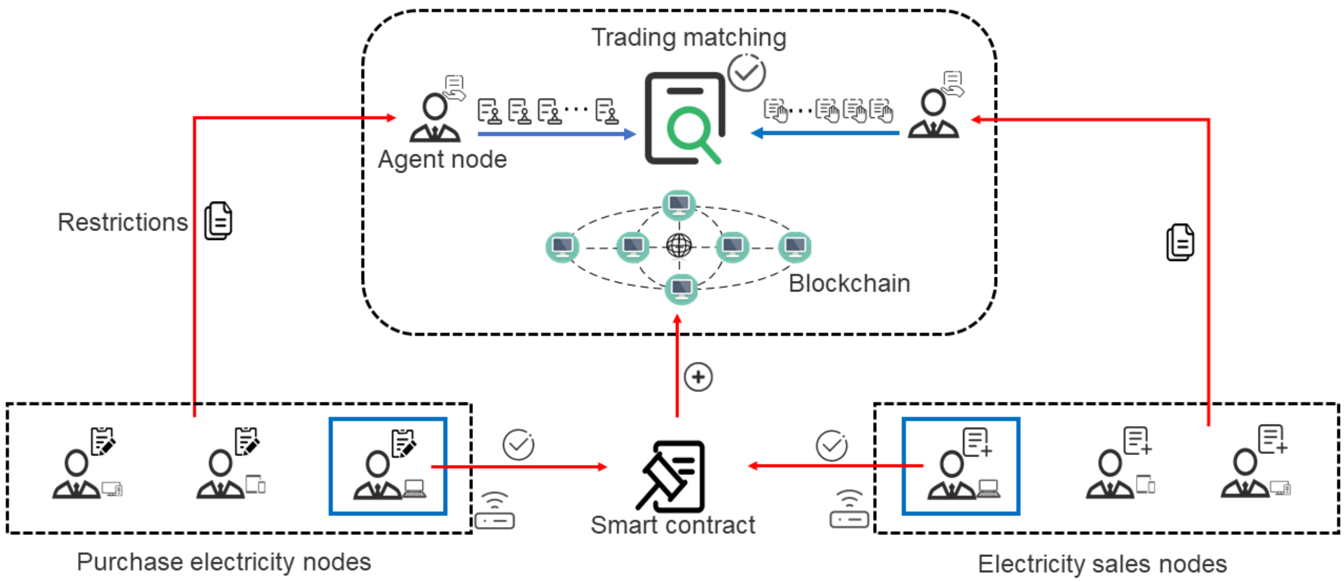

Figure 2: BC-TMS: Trading matching system model.

a lot of unnecessary overhead, thereby reducing the efficiency of the trading system. Finally, in order to find a trading object that meets the requirements, the transaction applicant has to broadcast his or her required information, and it is inevitable to disclose his private information. If there are malicious users in the system, they can use this information to disrupt the market. Using private information they can manipulate prices and cause the market to lose fairness. Our design goals are as follows:

- `Decentralized`: Facing the new pattern of energy production and the new trend of energy development, the traditional centralized energy production and marketing model cannot meet the current energy trading needs. It is imperative to promote the revolution in energy production and consumption. The system needs to design and implement a decentralized trading model in the context of large-scale access to distributed energy. With the continuous improvement of the degree of intelligence and digitization of the power grid, the number of smart terminal devices connected and the diversity of software are increasing significantly. The decentralized distributed energy trading model needs to ensure the security and credibility of the trading environment.
- `Trading matching`: The system needs to design a trading matching mechanism to match buyers and sellers to complete the transaction. The matching mechanism needs to be able to match supply and demand information effectively and intelligently based on different targets. At the same time, we also need to achieve high efficiency and low cost of trading matching to apply to the blockchain system. The trading matching mechanism should not only achieve reasonable matching, but also ensure that the interests of both buyers and sellers are maximized.
- `Privacy-preserving`: In order to improve usability and security, a distributed energy trading system based on blockchain needs to implement Privacy-preserving functions. The users involved in the trading inevitably need to publish their sensitive private information, such as price, electric power, and identity information, when looking for a transaction object. There is no doubt that trading users do not want their data to be exposed to all blockchain nodes. Secondly, the leakage of these private data will also bring security risks to the trading system. Assuming that there are malicious users in the system, they will collect the information to manipulate the electricity price and maliciously disrupt the fairness of the market. The matching mechanism needs to prevent this from happening.
- `Automatic execution`: Energy as a trading commodity has its special properties. The delivery of electrical energy cannot achieve instantaneous transmission, and

it is also difficult to achieve efficient storage. Therefore, the system needs to rely on contracts to achieve trading security and fairness. If there is no third-party intermediary agency to ensure the security, automation and transparency of the contract, it is difficult to achieve safe trading in a trustless environment. The system needs to support smart contract services that are automatically executed to ensure efficient, fast, and accurate energy trading.

- `High efficiency`: In a distributed energy trading system based on blockchain technology, the user nodes participating in the trading are generally lightweight computing devices, such as mobile phones and personal computers. Therefore, if the matching mechanism of the trading system requires too much computing power, general power users cannot participate. On the other hand, the matching algorithm needs to get results quickly. The delay of the matching mechanism needs to be controlled within the acceptable range of the trading.

3.2 Definition of System Model

In BC-TMS, all nodes in the blockchain are divided into two different types of entities according to their roles, including trading node and agent node.

- `Trading node`: Users of electric power trading participate in trading as nodes in the blockchain. They will set constraints based on their requirements for the transaction object as a reference for the matching mechanism.
- `Agent node`: We abstract a class of agent nodes in the blockchain. Their main job is to make the most reasonable match between buyers and sellers. At the same time, they also need to undertake the work of keeping accounts. At the end of each transaction cycle, they need to package, upload, and consensus on the transaction.

The system architecture of BC-TMS is shown in Fig 2. We proposed distributed energy trading matching mechanism based on blockchain is divided into five steps. The specific process is as follows.

step 1: The buyer sends a transaction request to the agent through the blockchain distributed network. In order to prevent false information from interfering with the transaction, the agent must check the buyer's identity and reputation. After passing the verification, the buyer submits the required attribute parameters of the matching object and the expected purchase price and other attribute requirements.

step 2: The agent node is obliged to verify the identity of the seller. After the verification is successful, the seller can submit attribute information such as electricity and price.

step 3: The agent node calculates the satisfaction of the buyer and the seller on each attribute based on the attribute values and priority calculation formulas provided by both parties, and establishes a transaction matching model.

step 4: According to the data provided by buyers and sellers, the network system first rejects matches that cannot meet each other's hard requirements. The agent node calculates the total satisfaction of both parties according to the model, on the basis of which the transaction prices of both parties are considered to calculate their own satisfaction, and the model is solved based on the satisfaction maximization to obtain the matching result.

step 5: The matching buyer and seller conduct business negotiations. If the negotiation is successful, the transaction is reached. At the same time, the agent node removes the information of the buyer and the seller and no longer participates in the matching; if the negotiation is unsuccessful, the next round of circulation is performed.

4 DESCRIPTION OF BC-TMS

In this section, we will introduce the details of the proposed distributed energy trading matching system based on blockchain.

4.1 Quantify satisfaction

Satisfaction is defined as the degree to which trading users like potential matching objects. Satisfaction is the comparison between the user's expected value and actual value. Now, we need to measure satisfaction with numbers. The satisfaction of trading users is also called the user satisfaction index. BC-TMS aims to maximize the satisfaction of both parties in the transaction, and at the same time consider the stable matching constraints, establish an optimization model and solve to obtain a matching scheme.

For energy trading, the buyer needs to consider multiple attributes of the transaction object, such as the price of electricity, electricity, and credibility. The buyer needs to submit two kinds of constraints to the agent node:

- `Hard constraints`: equal constraints, for example, the buyer requires the seller's credit qualification to be A-level.
- `Soft constraints`: non-equal sign constraints, have a certain range of attribute requirements. For example, the buyer requires the price of electrical energy to be within a certain range.

Therefore, the priority of matching is to satisfy the hard constraints first and then the soft constraints.

The attributes of trading users can be divided into income attributes and cost attributes.

- `Income attribute`: The larger the attribute value, the more profitable the attribute, that is, the larger the better attribute. In electric energy trading, general income-based attributes include credibility, number of transactions, electric power quality, and stability.
- `Cost attribute`: The smaller the attribute value, the more profitable the attribute. The cost attributes include electric power loss, default rate, and electric power price.

We set the trading user satisfaction interval to be represented by [0, 1], the maximum value of satisfaction is 1, and the minimum value is 0 (hard constraints are the primary condition for matching, and the quantification of satisfaction here only considers soft constraints).

For the income attribute, assuming the attribute's constraint condition is the interval (a, b), it is considered that the satisfaction value is 1 when the attribute value is greater than or equal to b, and the satisfaction value is 0 when the attribute value is less than or equal to a. For example, in the power trading, when the user's electric power loss is qualified as a, the electric power quality is good as b. If the constraint condition is a single-value $e_{\min}$, for example, it is required that the reputation value of the transaction party must be greater than the average value, then below the minimum value of the constraint, then the satisfaction is 0, and when the maximum value of the constraint (or the user's expected value) is reached, the satisfaction of the contracting party with this attribute is 1, and the difference is expressed in the middle.

For the cost-type attribute (the smaller the value, the better the attribute), assuming that the interval is (a, b), the satisfaction value of the attribute value is less than or equal to a is 1, and the satisfaction value is greater than or equal to b is 0. For example, the rate of power transmission is fast enough. If the time is less than a, the satisfaction is 1, and if the time is too long, the satisfaction is 0. If the constraint condition is a single value $e_{\max}$, for example, the failure rate is required to be less than 0.05, and then higher than the maximum value, the satisfaction is 0. When the minimum value (or the user's expectation value) is reached, the satisfaction of the sender with this attribute is 1, and the difference is expressed in the middle.

4.2 Trading matching

4.2.1 Apply for purchase. During the trading, the buyer provides the agent node with the hard constraint value of the relevant attribute. If the hard constraint is not met, the system automatically rejects the corresponding seller for the next round of matching. In addition to providing hard constraint values of relevant attributes to the agent node, the buyer must also submit soft constraint values to the intermediary. Because the buyer has different preferences for different attributes, it is necessary to submit the attribute preference. The system initially defaults that each attribute has the same weight.

1) Attribute satisfaction

The buyer sends the expected value E_{if} of the attribute f to the agent node. If the attribute f is a revenue attribute, the buyer must submit the minimum allowable value of the attribute E_{ifmin}. If the attribute f is a cost attribute, the maximum allowable value E_{ifmax} must be submitted.

Let B_i denote the i-th buyer node, f denote the attribute, S_j denote the seller node, and E_{jf} denote the value of the attribute f to be sold. When one party reaches the expectation value of the other party, $E_{if} = 1$, and other corresponding attribute values are calculated in proportion. When one party of the transaction fails to reach the acceptable range of the other party's soft constraint, it will be removed and the next round of circulation will be performed. Introducing the function $a_{ijf}(h_{jf})$ to express B_i's satisfaction with the software attribute f provided by S_j, then

For income attributes:

$$a_{ijf}(h_{jf}) = \begin{cases} 1, & h_{jf} \geq E_{if} \\ \frac{h_{jf} - E_{if\min}}{E_{if} - E_{if\min}}, & E_{if\min} \leq h_{jf} \leq E_{if} \end{cases}$$

If $h_{jf} - E_{if\min} < 0$, it will be directly eliminated and enter the next round.

For cost attributes:

$$a_{ijf}(h_{jf}) = \begin{cases} 1, & h_{jf} \leq E_{if} \\ \frac{E_{if\max} - h_{jf}}{E_{if\max} - E_{if}}, & E_{if} \leq h_{jf} \leq E_{if\max} \end{cases}$$

If $E_{if\max} - h_{jf} < 0$, it will be directly eliminated and enter the next round.

2) Attribute preference

The buyer can treat each attribute equally, and can also set the importance of each attribute corresponding to each soft constraint. This setting value is called the preference coefficient. Generally, the sender in software outsourcing sets different weights on its attributes. Let w denote the degree of preference, w_{if} denote the buyer B_i's preference coefficient for the attribute f, and the sum of the softwares attribute preference coefficients is 1.

$$\sum_{f=1}^{r_i} w_{if} = 1$$

Where $0 \leq w_{if} \leq 1$, r_i is the number of soft constraints that buyer e_i requires from the seller.

3) Total satisfaction expression

The evaluation result cannot be based on a certain attribute, but rather to evaluate the buyer s overall satisfaction. Use t_{ij} to express B_i's total satisfaction with S_j.

$$t_{ij} = \sum_{f=1}^{r_i} w_{if} a_{ijf}$$

4.2.2 Apply for sale. It is not difficult to imagine that the seller is most concerned about the selling price of electrical energy. Before the agent node performs the matching, the seller submits the desired selling price p_{sj}, the lowest selling price p_{sjmin}, and other attributes related to electric energy. Assuming that the seller s satisfaction is only related to the buyer B_i's bid p_{Bi}, the S_i's satisfaction with the contractor B_i is expressed as a function.

$$g_{ij} = \begin{cases} 1, & P_{Bi} \geq P_{Si} \\ \frac{P_{Bi} - P_{Si\min}}{P_{Sj} - P_{Sj\min}}, & P_{Sj\min} \leq P_{Bi} \leq P_{Sj} \end{cases}$$

4.2.3 Matching model. We set up a multi-objective transaction matching model with the goal of maximizing the total satisfaction of both parties. Let x_{ij} indicate whether the buyer B_i matches the seller S_j.

$$x_{ij} = \begin{cases} 1, & B_i \text{ match } S_j \\ 0, & B_i \text{ Mismatch } S_j \end{cases}$$

Buyer satisfaction:

$$\max \sum_{j=1}^{m} \left(\sum_{i=1}^{n} (x_{ij} t_{ij}) \right)$$

Seller satisfaction:

$$\max \sum_{j=1}^{m} \left(\sum_{i=1}^{n} (x_{ij} g_{ij}) \right)$$

4.2.4 Model solution. For both parties to the transaction, the agent nodes are treated with equal importance to ensure their fairness, and the average value of the satisfaction of both parties is selected for matching. Therefore, the multi-objective problem is transformed into the following single-objective model:

$$\max \sum_{j=1}^{m} \left(\sum_{i=1}^{n} (t_{ij} + g_{ij})\, x_{ij} \right)$$

The agent node can calculate the matching score of both parties through the above algorithm calculation. Based on the score, the agent node completes the precise matching between buyers and sellers.

5 SECURITY ANALYSIS

We will discuss the security of BC-TMS in this section. For system security assessment, we will conduct full analysis and description from the perspectives of trading security, privacy security, and matching security.

5.1 Trading security

In a distributed energy trading environment, the number of trading nodes is huge and the distribution range is wide. Facing the new energy production and marketing model, the traditional centralized exchange has a series of disadvantages such as low efficiency, high cost, and poor resistance to single-point attacks. In BC-TMS, we use blockchain as a distributed trading platform to ensure trading security while improving system efficiency. With its own technical characteristics, the blockchain can ensure the integrity of trading data [25]. The block is recorded in the chain after passing the consensus mechanism, and the trading data contained in the block cannot be tampered with maliciously. At the same time, we can trace back to any historical transaction record or contract to implement the audit function. The blockchain guarantees the security of trading data in the form of a distributed ledger, and solves the trust problem of distributed nodes by means of a consensus mechanism. It is not difficult to conclude that blockchain technology can achieve secure distributed energy trading.

5.2 Privacy-preserving

First, the blockchain uses pseudonyms to provide identity privacy protection for users participating in energy trading. The pseudonym serves as the unique identifier of the identity of the trading node and will not reveal the true identity of the users. At the same time, the system provides assistance services for seller nodes and buyer nodes participating in the trading by selecting trusted proxy nodes. The node directly sends its own trading information to the agent node to select the trading object. This approach avoids the disclosure of sensitive private information such as trading floor prices due to broadcast.

During the entire trading process of the system, the buyer and the seller cannot view the transaction information of any other node, and the privacy information of the trading node is fully protected. After the trading object matching procedure is completed, the node can still only obtain the node information recommended by the system to determine the trading intention.

5.3 Matching security

The entire trading matching of the system is a black box process. The matching is performed by the selected trusted agent node. The trading user cannot directly participate and can only obtain the matching result. This black box matching method not only protects user trading information but also ensures the security and credibility of the matching program[26][27].

6 APPLICABILITY ANALYSIS

With its strong technical advantages, the blockchain has developed rapidly. Blockchain technology has undergone a continuous leap from stage 1.0 to stage 3.0. Blockchain 1.0 is the basic version of blockchain technology, which can realize programmable currency and is a cryptocurrency application related to transfer, remittance and digital payment. Blockchain 2.0 proposes the concept of programmable finance, and the introduction of smart contracts has made it possible for the application of blockchain in the economic, market, and financial fields. Blockchain 3.0 can confirm, measure and store the property rights of every information representing value on the Internet, so that assets can be tracked, controlled and traded on the blockchain. At present, the application of blockchain has surpassed the financial field and entered many fields such as social notarization, Internet of Things, public services and intelligence. In [28], a privacy protection scheme for energy trading based on blockchain was proposed. In [29], blockchain is used in fog-based IoT services. It can be seen that the blockchain technology has been widely used in various fields.

Energy trading applications are not just conceptual, they are proven and deployed in communities and energy markets around the world including Australia, New Zealand, Europe and Asia. For instance, Brooklyn Microgrid (BMG) integrates emerging technologies and solutions such as blockchain and applies them to the energy and community solar fields. Sunchain integrates renewable energy and the digital world to develop an innovative application of solar energy based on blockchain. Pylon is a fast, scalable and lowest energy consumption blockchain project designed and developed in Spain specifically to meet the needs of the energy industry. Wepower is an energy trading platform based on blockchain technology, focusing on green energy. Currently, the platform operates in Australia and is open to certified commercial customers.

- `Brooklyn microgrid (BMG)` : The Brooklyn Microgrid was developed in 2016. The system is the first energy trading platform based on blockchain. Through blockchain technology and innovative solutions, BMG has developed Exergy, a licensed data platform that creates a localized energy market that enables energy trading between existing grid infrastructure. The BMG market allows producers (ie residential and commercial solar panel owners) to sell excess solar energy it produces to New York City residents who prefer to use renewable energy instead of fossil fuels. The application of the Brooklyn microgrid has led to a surge in solar energy production and consumption throughout New York City.
- `Sunchain`: Sunchain is an energy innovation application based on blockchain. Sunchain integrates renewable energy and the digital world to provide communities with new distributed energy trading services. Sunchain has proved through its IoT solution that it can achieve dynamically optimized solar energy distribution among different consumers. At the same time, on this blockchain, certification technology around electric power or energy sources is also in the process of further research and development.
- `Pylon`: In Pylon Network, Pylon has developed a neutral database based on blockchain technology to store consumption and production data for users in the energy market. Through the Pylon Network database, users (data owners) can control and decide with whom to share energy data, thereby actively participating in the market. With the help of the Pylon network, data neutrality can be achieved, and the innovation and competitiveness of the energy market can reach a new level. Consumers/producers can now use simple tools to decide how to handle their private information and can choose a third party (retailer or energy service company (ESCO)) that can access and provide the information to provide them with digital services.
- `Wepower`: Wepower was created to make the transaction and financing of green energy projects a simple process. WePower platform provides a streamlined and flexible renewable energy offtaker contracting solution, which saves time, effort and delivers higher returns to the renewable energy generation facility developers. It uses smart contracts to allow participants to fund new green energy projects or purchase their own green energy in an efficient, safe and transparent manner. It is also an international market where anyone can trade renewable energy. An important potential of Wepower is the integration with IoT technology, which will allow Internet-connected devices to buy and sell renewable energy through the use of smart contracts.

It is not difficult to conclude from the above case that the blockchain is constantly undergoing technological innovation, and there will be more distributed energy trading applications based on blockchain technology. Therefore, our proposed energy trading matching scheme based on blockchain BC-TMS has strong practical application significance.

7 CONCLUSION

This paper introduces a blockchain-based electrical energy trading system BC-TMS, introduces a matching algorithm to match users with the highest satisfaction of trading objects, and achieves reasonable and accurate matching between buyers and sellers. This design not only improves the fairness of the trading but also maximizes the benefits. At the same time, the system also provides a certain degree of privacy protection. The security and application analysis are conducted to prove the validity and practicability of our proposed scheme.

8 ACKNOWLEDGMENTS

The work is partially supported by the National Natural Science Foundation of China under Grant 61972148, Beijing Natural Science Foundation under grant 4182060.

REFERENCE

[1] Li Da Xu, Eric L. Xu, and Ling Li. Industry 4.0: state of the art and future trends. *International Journal of Production Research*, 56(7-8):2941–2962, 2018.

[2] Kun Wang, Jun Yu, Yan Yu, Yirou Qian, Deze Zeng, Song Guo, Yong Xiang, and Jinsong Wu. A survey on energy internet: Architecture, approach, and emerging technologies. *IEEE Systems Journal*, pages 1–14, 2017.

[3] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. *Future Generation Computer Systems*, page S0167739X17318332, 2017.

[4] Lu and Yang. Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, page S2452414X17300043, 2017.

[5] Keliang Zhou, Taigang Liu, and Lifeng Zhou. Industry 4.0: Towards future industrial opportunities and challenges. In *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2015.

[6] Pasquale Pace, Gianluca Aloi, Raffaele Gravina, Giuseppe Caliciuri, Giancarlo Fortino, and Antonio Liotta. An edge-based architecture to support efficient applications for healthcare industry 4.0. *IEEE Transactions on Industrial Informatics*, 15(1):481–489, 2019.

[7] Jay Lee, Hung An Kao, and Shanhu Yang. Service innovation and smart analytics for industry 4.0 and big data environment. *Procedia Cirp*, 16:3–8, 2014.

[8] Huang, A.Q., Crow, M.L., Heydt, G.T., Zheng, J.P., Dale, and S.J. The future renewable electric energy delivery and management (freedm) system: The energy internet. *Proceedings of the IEEE*, 2011.

[9] Y. Chai, C. Bai, C. Zhang, X. Han, X. Dai, and X. Jin. Energy internet system research based on development trend of urban energy system. In *2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2)*, pages 604–609, 2019.

[10] J. Li, Z. Zhou, J. Wu, J. Li, S. Mumtaz, X. Lin, H. Gacanin, and S. Alotaibi. Decentralized on-demand energy supply for blockchain in internet of things: A microgrids approach. *IEEE Transactions on Computational Social Systems*, 6(6):1395–1406, 2019.

[11] Kun Wang, Jun Yu, Yan Yu, Yirou Qian, Deze Zeng, Song Guo, Yong Xiang, and Jinsong Wu. A survey on energy internet: Architecture, approach, and emerging technologies. *IEEE Systems Journal*, pages 1–14, 2017.

[12] Kun Wang, Huining Li, Yixiong Feng, and Guangdong Tian. Big data analytics for system stability evaluation strategy in the

energy internet. *IEEE Transactions on Industrial Informatics*, 13(4):1969–1978, 2017.

[13] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. Ashiqur Rahman. Blockchain-based charging coordination mechanism for smart grid energy storage units. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 504–509, 2019.

[14] Y. Wang, Z. Su, and N. Zhang. Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network. *IEEE Transactions on Industrial Informatics*, 15(6):3620–3631, 2019.

[15] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, and N. Zhang. A secure charging scheme for electric vehicles with smart communities in energy blockchain. *IEEE Internet of Things Journal*, 6(3):4601–4613, 2019.

[16] S. Wang, A. F. Taha, J. Wang, K. Kvaternik, and A. Hahn. Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(8):1612–1623, 2019.

[17] N Wang, X Zhou, X Lu, Z Guan, L Wu, X Du, and G Mohsen. When energy trading meets blockchain in electrical power system: The state of the art. In *Applied Sciences 9.8 (2019): 1561*. MDPI, 2019.

[18] Jiawen Kang, Yu Rong, Xumin Huang, Sabita Maharjan, Zhang Yan, and Ekram Hossain. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics*, 13(6):3154–3164, 2017.

[19] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao, and C. Lin. Applying blockchain technology to decentralized operation in future energy internet. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–5, 2017.

[20] Esther Mengelkamp, Benedikt Notheisen, Carotin Beer, David Dauer, and Christof Weinhardt. A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science Research & Development*, 33(1-2):207–214, 2018.

[21] S. Seng, C. Luo, X. Li, H. Zhang, and H. Ji. User matching on blockchain for computation offloading in ultra-dense wireless networks. *IEEE Transactions on Network Science and Engineering*, pages 1–1, 2020.

[22] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy (SP)*, 2016.

[23] Liang Wei, Zhiguo Ding, Yonghui Li, and Lingyang Song. User pairing for downlink non-orthogonal multiple access networks using matching algorithm. *IEEE Transactions on Communications*, PP(99):1–1, 2017.

[24] Mohammad Akbarpour, Shengwu Li, and Shayan Oveis Gharan. Thickness and information in dynamic matching markets. *Social Science Electronic Publishing*, 128(3):783–815, 2020.

[25] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. *Cacm*, 47(6):53–57, 2008.

[26] Xianfeng Gao, Yu an Tan, Hongwei Jiang, Quanxin Zhang, and Xiaohui Kuang. Boosting targeted black-box attacks via ensemble substitute training and linear augmentation. *Applied ences*, 9(11):2286, 2019.

[27] Yuan Xue, Yu-an Tan, Chen Liang, Yuanzhang Li, Jun Zheng, and Quanxin Zhang. Rootagency: A digital signature-based root privilege management agency for cloud terminal devices. *Information Sciences*, 444:36–50, 2018.

[28] Xin Lu, Zhitao Guan, Xiao Zhou, Longfei Wu, and Mohsen Guizani. An efficient and privacy-preserving energy trading scheme based on blockchain. In *GLOBECOM 2019 - 2019 IEEE Global Communications Conference*, 2019.

[29] K. Lei, M. Du, J. Huang, and T. Jin. Groupchain: Towards a scalable public blockchain in fog computing of iot services computing. *IEEE Transactions on Services Computing*, 13(2):252–262, 2020.